Yee &
Associates, P.C.

4100 Alpha Road
Suite 1100
Dallas, Texas 75244

Main No. (972) 385-8777
Facsimile (972) 385-7766

Facsimile Cover Sheet

To: Commissioner for Patents for **Examiner Linh L. D. Son** **Group Art Unit 2135**	Facsimile No.: **571/273-8300**
From: Jane M. Roberts Legal Assistant to James O. Skarsten	No. of Pages Including Cover Sheet: **35**

Message:

Enclosed herewith:

- Transmittal Document; and
- Appeal Brief.

Re: Application No. **09/810,288**
     Attorney Docket No: **CA920000054US1**

Date: Tuesday, August 23, 2005

Please contact us at (972) 385-8777 if you do not receive all pages indicated above or experience any difficulty in receiving this facsimile.	*This Facsimile is intended only for the use of the addressee and, if the addressee is a client or their agent, contains privileged and confidential information. If you are not the intended recipient of this facsimile, you have received this facsimile inadvertently and in error. Any review, dissemination, distribution, or copying is strictly prohibited. If you received this facsimile in error, please notify us by telephone and return the facsimile to us immediately.*

PLEASE CONFIRM RECEIPT OF THIS TRANSMISSION BY FAXING A CONFIRMATION TO 972-385-7766.

RECEIVED
IN THE UNITED STATES PATENT AND TRADEMARK OFFICE CENTRAL FAX CENTER

AUG 2 3 2005

In re application of: **Kou et al.**	§	Group Art Unit: **2135**
	§	
Serial No.: **09/810,288**	§	Examiner: **Son, Linh L. D.**
	§	
Filed: **March 16, 2001**	§	Attorney Docket No.: **CA920000054US1**
	§	
For: **Secure Session Management and** **Authentication for Web Sites**	§	

36736
PATENT TRADEMARK OFFICE
CUSTOMER NUMBER

TRANSMITTAL DOCUMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:
ENCLOSED HEREWITH:

• Appeal Brief (37 C.F.R. 41.37)

A fee of $500.00 is required for filing an Appeal Brief. Please charge this fee to IBM Corporation Deposit Account No 09-0461. No additional fees are believed to be necessary. If, however, any additional fees are required, I authorize the Commissioner to charge these fees which may be required to IBM Corporation Deposit Account No 09-0461. No extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and I authorize the Commissioner to charge any fees for this extension to IBM Corporation Deposit Account No 09-0461.

Respectfully submitted,

James O. Skarsten
James O. Skarsten
Registration No. 28,346
Duke W. Yee
Registration No. 34,285
YEE & ASSOCIATES, P.C.
P.O. Box 802333
Dallas, Texas 75380
(972) 385-8777
ATTORNEYS FOR APPLICANTS

Docket No. CA920000054US1   *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Kou et al.	§	
	§	Group Art Unit: 2135
Serial No. 09/810,288	§	
	§	Examiner: Son, Linh L.D.
Filed: March 16, 2001	§	
	§	
For: Secure Session Management	§	
and Authentication for Web Sites	§	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF (37 C.F.R. 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on June 23, 2005.

The fees required under § 41.20(B)(2), and any required petition for extension of time for filing this brief and fees therefore, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

(Appeal Brief Page 1 of 33)
Kou et al.— 09/810,288

PAGE 3/35 * RCVD AT 8/23/2005 4:55:33 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/26 * DNIS:2738300 * CSID:972 385 7766 * DURATION (mm-ss):08-00

REAL PARTY IN INTEREST

The real party in interest in this appeal is the following party: International Business Machines Corporation.

RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-34

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims canceled: 32 and 34
2. Claims withdrawn from consideration but not canceled: NONE
3. Claims pending: 1-31 and 33
4. Claims allowed: NONE
5. Claims rejected: 1-31 and 33
6. Claims objected to: NONE

C. CLAIMS ON APPEAL

The claims on appeal are: 1-31 and 33

STATUS OF AMENDMENTS

An amendment to the claims filed subsequent to the Final Rejection was not entered.
Therefore, Claims 1-31 and 33 on appeal herein are as amended in the Response to Office
Action filed October 14, 2004.

(Appeal Brief Page 5 of 33)
Kou et al.– 09/810,288

SUMMARY OF CLAIMED SUBJECT MATTER

A.   CLAIM 1 - INDEPENDENT

The subject matter of Claim 1 is directed to a method of secure management and authentication between a web site and a web client, such as website 20 and web client 16 shown in Figure 1. The web site 20 has both secure web pages 32 and non-secure web pages 34, as shown by Figure 1 and taught at page 8, lines 6-9 of Applicants' specification. Steps of the method specify that a non-secure communication protocol and a session cookie are to be used, when a client requests access to non-secure web pages, and a secure communication protocol and an authcode cookie are to be used, when a client requests access to web pages. These steps of Claim 1 are supported by the application such as at page 5, lines 11-16. In addition, Claim 1 teaches that use of authcode cookies (for secure web pages) is interspersed between use of session cookies (for non-secure web pages). This Claim 1 feature is particularly supported at page 5, lines 20-22. Features of Claim 1 are additionally supported by steps 194 and 202-212 of Figure 6A.

B.   CLAIM 12 – INDEPENDENT

The subject matter of Claim 12 is directed to a system for secure management and authentication between a web site and a web client. The system comprises a web server, having a web site and a web client coupled to the web server via a communication channel, wherein the web site includes secure and non-secure web pages. These elements of Claim 12 are supported in the application such as at Figure 1, which shows a communication channel 14 coupling a web server 12 to a web client 16, and a web site 20 of web server 12 includes secure web pages 32 and non-secure web pages 34. The above elements are further supported at page 6, line 24 through page 7, line 20 and page 8, lines 6-9 of Applicants' specification. Claim 12 further discloses that the web site includes a non-secure communication protocol and a session cookie that is used for allowing web client access to each one of the non-secure web pages and, a secure communication

protocol and an authcode cookie that is used for allowing web client access <u>only</u> to the secure web pages. These features of Claim 12 are supported in the application such as at page 5, lines 11-22, and steps 152-174 of **Figure 5B**, together with the application at page 24, line 26 through page 25, line 15.

C.   **CLAIM 20 – INDEPENDENT**

The subject matter of Claim 20 is directed to a computer program product in a computer readable medium for presenting content in a document. The claim is a computer program product counterpart claim to method Claim 1.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A.   GROUND OF REJECTION 1 (Claims 12-17)

Claims 12-17 stand rejected under 35 U.S.C. § 102(b) as anticipated by U.S. Patent No. 5,966,705 (Koneru et al.).

B.   GROUND OF REJECTION 2 (Claims 1-7, 10-11, 20-26 and 29-30)

Claims 1-7, 10-11, 20-26 and 29-30 stand rejected under 35 U.S.C. § 102(b) as anticipated by U.S. Patent No. 5,966,705 (Koneru et al.).

C.   GROUND OF REJECTION 3 (Claims 8-9, 18-19, 27-28, 31 and 33)

Claims 8-9, 18-19, 27-28, 31 and 33 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,966,705 (Koneru et al.) in view of U.S. Patent No. 6,092,196 (Reiche).

ARGUMENT

A.   GROUND OF REJECTION 1 (Claims 12-17)

Claims 12-17 stand rejected under 35 U.S.C. § 102(b) as anticipated by U.S. Patent No. 5,966,705 (Koneru et al.).

A.1.   Teachings and Purpose of Applicants' Claim 12

In making their invention, Applicants were concerned with communication between a web client and a web site having both secure and non-secure web pages. Applicants recognized that for web sites such as e-commerce web sites, it is necessary to allow for authentication and session management when holding a conversation with a web client. Session management enables a web site to remember a web client between different login sessions, whereas authentication is a security measure which assures a web site that a request came from the same web client who originally logged onto the web site.

As is well known to those of skill in the art, cookies are a popular method for session management between a web site and a web client. For non-secure web pages, communication protocol encrypts the data transmitted between the e-commerce web site and a web client. Authentication and session management may be carried out by utilizing HTTP Basic Authentication, Name-Value Pair Authentication, or session cookies. However, for secure web pages, cookie based session management must incorporate a secure communication protocol, to prevent unauthorized users from stealing sensitive data contained in the cookie. One such protocol is HTTPS (HTTP/SSL), described hereinafter in further detail.

The above teachings of Applicants are set forth in the present application, such as at page 1, line 24-page 2, line 6, and page 3, lines 17-22 and page 5, lines 1-9 and 11-15, as follows:

> To correct these problems, an e-commerce web site must allow for authentication and session management while holding a conversation with a web client. Further, a secure communication protocol must be used when sensitive information is transmitted between the web client and the

e-commerce web site.   Session management allows a web site to remember a web client between different login sessions whereas authentication is a security measure which assures a web site that a request came from the same web client who originally logged onto the web site. A secure communication protocol encrypts the data transmitted between the e-commerce web site and a web client. To accomplish authentication and session management, one may utilize HTTP Basic Authentication, Name-Value Pair Authentication or session cookies.

Cookie based session management must incorporate a secure communication protocol to prevent unauthorized users from stealing sensitive data contained in the cookie. One such protocol is HTTPS (HTTP over SSL). The acronym SSL stands for Secure Socket Layer protocol which is an industry standard for transmitting information securely while using HTTP. HTTPS includes provisions for web server authentication (verifying the web server's identity to the web client), data encryption and web client authentication (verifying the web client's identity to the web server).

Furthermore, switching between HTTP and HTTPS can be troublesome because currently when a web client logs onto a web site using HTTPS, a cookie is issued to authenticate the web client, however, if the web client later browses a non-secure web page at the web site using HTTP, the same cookie is sent to the web client in clear text. At this point an unauthorized user can steal the cookie. Thus, using a single cookie under these circumstances jeopardizes the security of the web site.

Accordingly, there is a need for an improved secure session management and authentication method, using cookies, to protect both the web site and the web client from unauthorized users. The present invention addresses these needs.

The present invention provides a method for secure session management and authentication between a web site and a web client, the web site having secure and non-secure web pages, the method having the steps of utilizing a non-secure communication protocol and a session cookie when the web client requests access to non-secure web pages; and utilizing a secure communication protocol and an authcode cookie when the web client requests access to secure web pages.

As indicated in the application at page 5, lines 1-6, Applicants recognized that there are significant problems in switching between a secure protocol such as HTTPS and a non-secure protocol such as HTTP, while using only a single type of cookie. For example, switching between HTTPS and HTTP can be troublesome in that when a web

client logs on to a web site using HTTPS, a cookie is issued to authenticate the web client. If the web client later browses a non-secure page at the web site using HTTP, the same cookie is sent to the web client in clear text. At this point an unauthorized user can steal the cookie. Thus, using a single cookie in this situation, even if it is a secure cookie, can jeopardize the security of the web site. This is even more likely to happen when a user is continually switching between secure and non-secure web pages.

Applicants overcome the above drawbacks and disadvantages of the prior art by means of their invention, as set forth in Claim 12. Claim 12 provides that both different cookies and different protocols are to be used, depending on whether access is requested to secure or non-secure web sites. More particularly, Claim 12 recites that a secure cookie and protocol are to be used only to access secure web pages, whereas a non-secure cookie and protocol are to be used to access non-secure web pages. Claim 12 of Applicants' invention, in its present form, reads as follows:

> 12.   A system, for secure session management and authentication between a web site and a web client, said system comprising a web server, a web client and a communication channel, said web server coupled to said web client via said communication channel, said web server having a web site, said web site including:
> a) secure and non-secure web pages;
> b) a non-secure communication protocol and a session cookie for allowing said web client access to each one of said non-secure web pages; and
> c) a secure communication protocol and an authcode cookie that is used for allowing said web client access only to said secure web pages.

A.2.   Rejection of Claim 12 by Examiner

In a Final Office Action dated January 25, 2005, the Examiner stated the following:

> 2.   Claims 1-7, 10-17, 20-26, and 29-30 are rejected under 35 U.S.C. 102(b) as being anticipated by Koneru et al, US Patent No. 5966705, hereinafter "Koneru".
> As per claim 1-7, 10-17, 20-26, and 29-30, the previous rejection is maintained. Further, Koneru does teach clearly that "the utilizations of said authcode are interspersed between utilizations of said session cookie,

and at least some utilizations of said session cookie take place after
utilizations of said authcode cookie" in (Col 7 line 22 to Col 8 line 35).
The GUID (Col 5 lines 20-25) is utilized in the public area get switched
with the user identification entered by the user as the key in the private and
secured areas (Col 7 lines 56-67). In additional, the user must acquire the
GUI token prior entering the private and secure areas (Col 8 lines 25-36).

Final Office Action dated January 25, 2005, page 2

7.   In regarding to Konerus' invention, even though the authcode
cookie and the session cookie is one cookie, but it still anticipated the
claimed invention. The name is given to the cookie to distinguish two
different applications. However, it is shown clearly that both cookies can
be as one to maintain the authenticated data neatly. Even though, the
cookie is in clear text format, but it does have the capability to have the
cookie authenticate in the SSL communication pipe (Col 6 lines 38-44) to
prevent unauthorized user read the cookie during the switching between
secure and non-secure web pages. Further nowhere in claim language
recites the limitations in the first paragraph on page 11 of the remark and
clearly explains otherwise.

Final Office Action dated January 25, 2005, page 4

In an Advisory Action dated May 6, 2005, the Examiner stated the following:

Response to Arguments
        Regarding to the argument on last paragraph on page 14,"(1) The
authcode cookie is used only to allow the web client to access secure web
pages." (Recited in claim 12); this feature does teach by Koneru et al, US
Patent No. 5966705, hereinafter "Koneru" in column 7 lines 55-60.
Eventhough, the GUID does utilize in both public and private area, the
actual GUID is only allow the secure server to identify the first level of
authentication, which is the userID. With the recognition of the user ID,
the server verifies the password and then totally replaces the GUID as the
key with the user Identification entered to get access in the secure area.
The New GUID that is a new GUID including the user identification
entered by the user (Col 7 lines 50-65, and Col 8 lines 10-14). Therefore,
claim 12 rejection is maintained.

Advisory Action dated May 6, 2005, page 2

The above statements of the Examiner appear to be the statements most pertinent

to Applicants' Claim 12. These statements cite sections of Koneru at col. 5, lines 20-25;

col. 6, lines 38-44 and col. 7, line 22 through col. 8, line 36. Each of these sections is set forth below:

<div align="center">

Col. 5, lines 20-25

</div>

Client Identifier

When the client computer 20 connects to the server 58, a token, such as a GUID, is assigned to the client and stored locally as a client identifier (not shown), often called a "cookie," as is further described below. A database entry is also created and stored on the server computer 58 to track

<div align="center">

Col. 6, lines 38-44

</div>

secure

If this attribute is set, the client identifier is transmitted from user client 20 only if the communication channel with server 58 is secure (e.g., utilizing a secure socket layer). If this attribute is not specified, the client identifier is sent regardless of the security of the channel.
Method of Tracking Prior to Entering the Secure Area

<div align="center">

Col. 7, line 22 through col. 8, line 36

</div>

Process block 90 indicates actions taken by the server when the user accesses a private area on the server 58. The server 58 checks the database entry associated with the user by using the GUID as a key, as described above. The server then checks a registration field in the database entry that indicates whether the user has previously registered. If the user has not registered, the user must go through a registration process. Usually the registration process requires the user to enter personal information or requires the user to answer questions. After having registered, the registration field in the database is changed to indicate that the user has now registered. If the user leaves the private area and returns, the server 58 again checks the database entry and determines that the user has already registered. As a result, the user is given automatic access to the private area without further registration. Such registration checking is transparent to the user.

Process block 92 indicates actions taken when the user tries to access a secure area on the server 58. The server 58 displays a document to the user that requests a user identification and password. Additionally, if the user has not previously entered a user identification and password, the user is offered a sign-up process through which the user must pass in order to enter the secure area. If the user previously entered a user identification and password, it is stored in the database entry. Upon entering the proper user identification and password, the server 58 compares the user-entered user identification and password to that stored in the database entry. Only if the two match, is the user allowed to access the secure area.

Steps Taken upon Entering the Secure Area

FIG. 4 shows additional steps in the method of tracking 80 after the user accesses the secure area. Process block 96 shows that the server 58 receives the user identification entered by the user.

Process block 98 shows that the server no longer uses the GUID as the key to the database entry. Instead, the GUID is replaced as the key with the user identification entered by the user.

Process block 100 shows that the user identification and the GUID are both stored in the client identifier or cookie on the client computer 20. The user identification can be stored in the "name=VALUE" attribute described above. Alternatively, the user identification can be stored in other attributes described above or other attributes can be created for storing the user identification.

Process block 102 indicates that the GUID is separately stored in a field within the database entry. This field is used for a comparison with the GUID subsequently sent from the client computer 20, as is further described below.

Method of Tracking after Entering the Secure Area

FIG. 5 shows the tracking method 80 as a user enters public, private and secure areas after the key is switched from the GUID to the user identification.

Process block 106 indicates that the user is browsing a public, private or secure area after having previously entered a secure area.

Process block 108 indicates that the client 20 passes the client identifier, which includes the GUID and the user identification, to the server 58.

Process block 110 indicates that the server 58 uses the user identification as a key to accessing the database entry associated with the user. Thus, user information stored in a database entry can be accessed to provide customized content to the user or additional information about the user's browsing characteristics can be stored in the database entry. The database entry also has a field that includes a GUID which is stored as shown in process block 102 (FIG. 4).

Process block 112 indicates that the GUID stored in the client identifier and received from the client is compared to the GUID stored in the database entry.

Process blocks 114 and 116 represent actions taken by the server 58 in the public and private areas, respectively. In both process blocks 114 and 116, if the GUID's checked in process block 112 are equivalent, the user is provided customized content that is stored in the database entry. If the GUIDs are different, the user is either presented with an error or generic, uncustomized content. Thus, a heightened level of authentication is achieved by ensuring that the user's customized data is not displayed unless the check shows that the user is genuine.

Process block 118 shows that the user must still enter a user identification and password to enter the secure area.

A.3.   Analysis of Koneru et al. Reference

A prior art reference anticipates a claimed invention under 35 U.S.C. § 102 only if every element of the claimed invention is identically shown in that single reference, arranged as they are in the claims. *In re Bond,* 910 F. 2d 831; 832, 15 U.S.P.Q. 2d 1566, 1567 (Fed Cir. 1990). All limitations of the claimed invention must be considered when determining patentability. *In re Lowry,* 32 F. 3d 1579, 1582, 21 U.S.P.Q. 2d 1031, 1034 (Fed Cir. 1994). Anticipation focuses on whether a claim reads on the product or process a prior art reference discloses, not on what the reference broadly teaches. Kalman v. Kimberly-Clark Corp., 713 F. 2d 760, 218 U.S.P.Q. 781 (Fed Cir. 1983).

Applicants respectfully submit that Koneru does not teach every element of the claimed invention arranged as they are in Claim 12. Specifically, Koneru does not teach, in the over-all combination of Claim 12, a secure communication protocol and an authcode cookie that is used for allowing a web client access only to secure web pages.

Moreover, it is a fundamental principle of patent law that prior art must be considered in its entirety. MPEP 2141.02. Accordingly, the following additional sections of Koneru are set forth and discussed below: col. 2 lines 48-62; col. 6, lines 55-61; the Koneru abstract; claim 1 of Koneru; and Figure 5.

Very pertinent teachings of the Koneru reference are set forth in the abstract thereof, which reads as follows:

> A system and method is disclosed for tracking a user across both secure and non-secure areas on an Internet and/or Internet site. In one aspect of the system and method, when a user first accesses a non-secure area, such as a public area, the user is assigned a token, such as a globally-unique identifier (GUID). The token is used as a key to a database entry on a server computer for tracking the user in non-secure areas. When the user first accesses a secure area, the user is prompted to enter a user identification and a password. The user identification is then used as a key to the database entry, rather than the token. The server then uses the user identification to track the user across both secure and non-secure areas. (Emphasis added.)

This teaching is further emphasized in the Koneru specification, such as at column 6, lines 55-61, and at claim 1 of Koneru, which respectively read as follows:

Using the present invention, the method of tracking a user depends upon whether the user has accessed a secure area 78. Prior to accessing a secure area 78, the server 58 tracks the user based upon the GUID stored in the client identifier on the client computer 20. After the user has accessed the secure area 78, the system tracks the user based upon a user identifier entered by the user. (Emphasis added.)

1. A method of tracking a user on a client computer as the user accesses secure and non-secure areas on a network server computer, comprising the steps of:
upon first accessing a non-secure area, assigning a token representing the user wherein the token does not contain a user identification and using the token as a key for accessing a database entry associated with the user on the server computer;
upon first accessing the secure area, receiving a user identifier associated with the user;
after accessing the secured area, replacing the token with the user identification as the key to the database entry; and
the database entry including customization information associated with user. (Emphasis added.)

From the above statements set forth in the Koneru reference, it is abundantly clear that when the user first accesses a non-secure area on a server, the user is assigned a token, or a GUID. The token is used as an access key for non-secure areas only until the first time that the user accesses a secure area. Thereupon, the token is replaced with a user identification. From then on, the user identification is used as the access key for both secure and non-secure areas.

To the extent that there is any equivalency or correspondence between Applicants' Claim 1 and the Koneru disclosure, the session cookie of Claim 1 would correspond to the token or GUID of Koneru, and the authcode cookie of Claim 1 would correspond to the user identification of Koneru. In view of this, Applicants respectfully submit that Koneru cannot teach every element of Claim 12, arranged as recited therein. Specifically, Koneru does not teach the above Claim 12 feature of an authcode cookie that is used for allowing web client access only to secure web pages. This feature of Claim 12 is, of course, essential for Applicants' purpose. In contrast, Koneru emphasizes repeatedly that the user identification is to be used to access both secure areas and non-secure areas. In

addition to the Koneru sections referred to above, this characteristic is explicitly taught in Koneru at col. 2, lines 48-62, and particularly at lines 60-62:

> In one aspect of the invention, when a user first accesses a non-secure area on a site, such as a public area, the user is assigned a token, such as a GUID, that uniquely represents the user. The token is used as a key to a database entry associated with the user on the site, as described above. When the user first accesses a secure area on the same site, the user is prompted to enter a user identification and a password. After receiving this information, the site uses the user identification, rather than the token, as the key to the database entry across both non-secure and secure areas. The user identification is then stored in a cookie and is received by the site each time the client computer passes the cookie to the site. Thus, using the user identification as a key, only one database entry is needed to track users across both non-secure and secure areas. (Emphasis added).

Clearly, the user identification of Koneru, equivalent to the authcode cookie of Claim 12, is not used to allow client access only to secure web pages, as is required by the recitation of Applicants' Claim 12.

Applicants consider that the respective Koneru citations contained in the Examiner's statements, as previously set forth, either support or are consistent with the Koneru teachings described above. Thus, in the cited Koneru section at col. 7, line 22 through col. 8, line 36, it is stated at col. 7, lines 57-59 that "Process block 98 shows that the server no longer uses the GUID as the key to data entry. Instead, the GUID is replaced as the key with the user identification". (Emphasis added.) This disclosure clearly supports the teachings of Koneru discussed above, such as at col. 2, lines 60-62.

Col. 8, lines 6-36 is directed to Figure 5, which is shown below:

FIG. 5

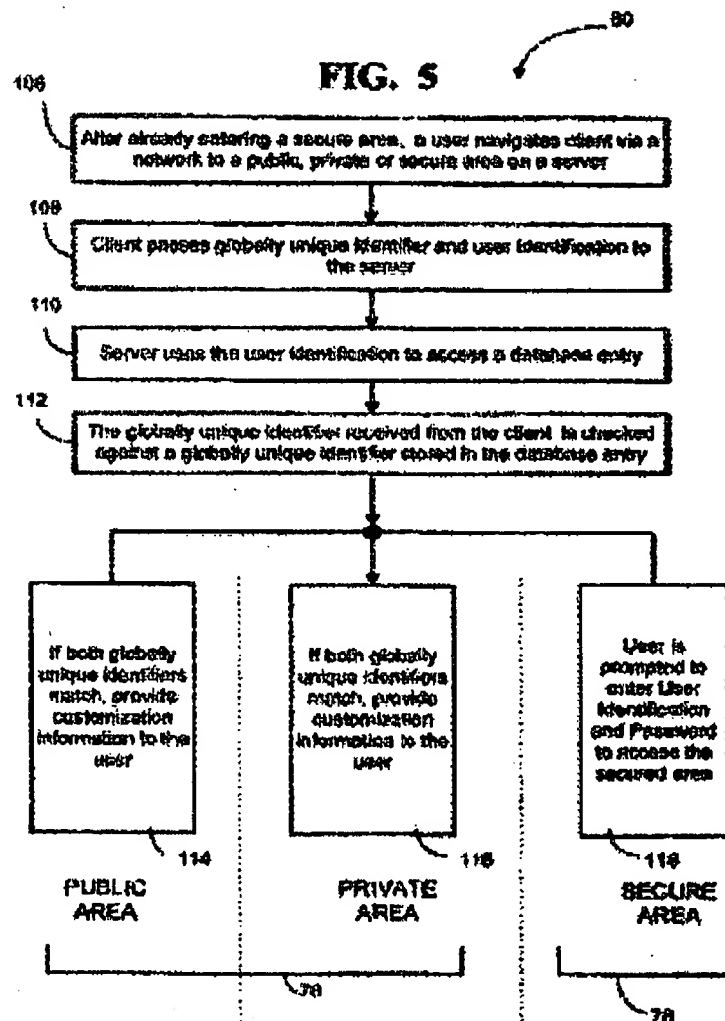
80
106
After already entering a secure area, a user navigates client via a network to a public, private or secure area on a server
108
Client passes globally unique identifier and user identification to the server
110
Server uses the user identification to access a database entry
112
The globally unique identifier received from the client is checked against a globally unique identifier stored in the database entry
If both globally unique identifiers match, provide customization information to the user
If both globally unique identifiers match, provide customization information to the user
User is prompted to enter User Identification and Password to access the secured area
114
116
118
PUBLIC AREA
PRIVATE AREA
SECURE AREA
76
78

Figure 5 of Koneru, together with col. 8, lines 6-36 thereof, shows an arrangement having both a non-secure area 76 and a secure area 78. Figure 5 further shows that public and private areas of non-secure area 76 are accessed using the GUID of Koneru. This is apparently done to provide "a heightened level of authentication", as taught at col. 8, lines 31-32. However, Figure 5 of Koneru shows very clearly that before the GUID can be used to access a non-secure area, database entry must first be provided by the user identification. This is taught by process block 110 of Figure 5, which states that "Server uses the user identification to access a database entry." (Emphasis added.) Thus, process block 110

clearly teaches that in the arrangement of Figure 5, access to both the secure and non-secure areas requires use of the user-identification.

In view of this disclosure, it is readily apparent that Figure 5 of Koneru and its associated text teach away from Applicants' Claim 12 recitation of an authcode cookie, associated with security, for allowing access only to secure web pages. In the Figure 5 arrangement of Koneru, the user identification, associated with security, must always be used in order to allow access to non-secure area 76.

At col. 5, lines 20-25 of Koneru the GUID is referred to as a token stored as a client identifier. Col. 6, lines 38-44 apparently pertains to transmission of the GUID or client identifier, prior to entering a secure area. Koneru citations at col. 7, lines 55-65 and col. 8, lines 10-14 appear to emphasize that the GUID and user identification are distinct entities. Accordingly, these citations are each considered to support or to be consistent with conclusions regarding Koneru, as discussed above.

Koneru, at col. 7, lines 52-60, pertains to Figure 4 thereof. Applicants consider that the citation to col. 7, lines 52-60 likewise supports the above conclusions regarding Koneru.

A.4.   Conclusion

For at least all of the above reasons, Applicants respectfully submit that Koneru et al. does not teach or suggest all of the features of Claim 12.

At least by virtue of their dependency on Claim 12, Koneru et al. does not teach or suggest the features of dependent Claims 13-17.

Accordingly, it is respectfully requested that the Board reverse the Examiner's final rejection of Applicants' Claims 12-17.

B.   GROUND OF REJECTION 2 (Claims 1-7, 10-11, 20-26 and 29-30)

Claims 1-7, 10-11, 20-26 and 29-30 stand rejected under 35 U.S.C. § 102(b) as anticipated by U.S. Patent No. 5,966,705 (Koneru et al.).

(Appeal Brief Page 19 of 33)
Kou et al.– 09/810,288

PAGE 21/35 * RCVD AT 8/23/2005 4:55:33 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/26 * DNIS:2738300 * CSID:972 385 7766 * DURATION (mm-ss):08-00

1.   A method of secure session management and authentication between a web site and a web client, said web site having secure and non-secure web pages, said method comprising the steps of:
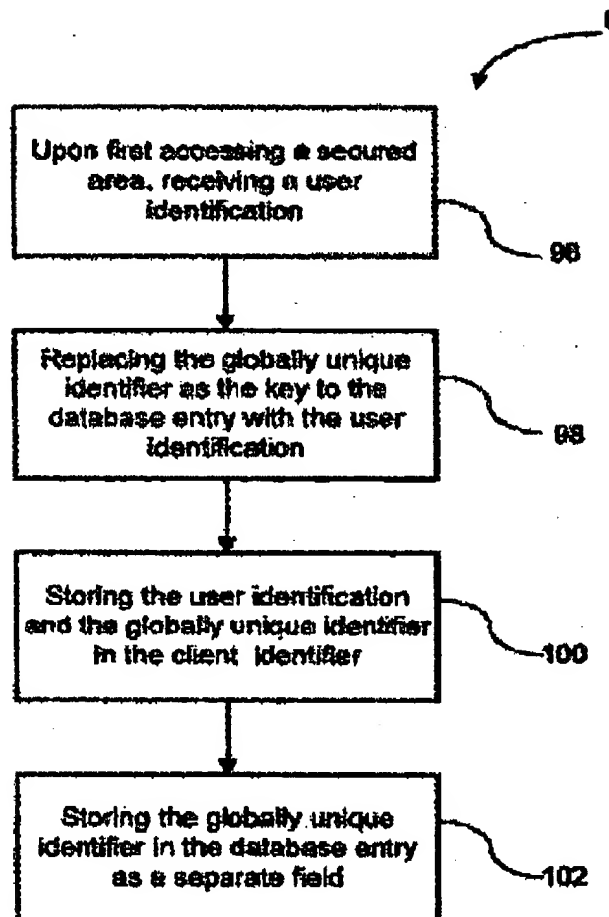a) utilizing a non-secure communication protocol and a session cookie when said web client requests access to said non-secure web pages;
b) utilizing a secure communication protocol and creating an authcode cookie when said web client requests access to said secure web pages, so that utilizations of said authcode cookie are interspersed between utilizations of said session cookie, and at least some utilizations of said session cookie take place after utilizations of said authcode cookie.

B.1.   Distinguishing Features of Claim 1

Applicants' Claim 1 is considered to distinguish over the Koneru reference, particularly in reciting, in the over-all combination of Claim 1, utilizations of the authcode cookie that are interspersed between utilizations of the session cookie. As discussed above, Koneru repeatedly emphasizes a different arrangement, whereby a token referred to as a GUID is used to access non-secure areas only until the first time that the user accesses a secure area. Thereupon, the token is replaced with a user identification, which is used thereafter to access both secure and non-secure areas. This teaching of Koneru, discussed above in connection with the Koneru abstract, col. 6, lines 55-61 and col. 7, lines 57-60, directs away from the Claim 1 feature of authcode utilizations interspersed between session cookie utilizations.

B.2.   Analysis of Cited Koneru Sections

As indicated by statements of the Examiner in the Final Office Action, as set forth above, the principal section of Koneru cited against Applicants' Claim 1 is at col. 7, line 22 through col. 8, line 36. Koneru at col. 7, lines 52-67 pertains to Figure 4 thereof, and col. 8, lines 1-36 pertains to Figure 5. Figure 4 is shown below:

(Appeal Brief Page 20 of 33)
Kou et al.— 09/810,288

PAGE 22/35 * RCVD AT 8/23/2005 4:55:33 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/26 * DNIS:2738300 * CSID:972 385 7766 * DURATION (mm-ss):08-00

FIG. 4

```
┌──────────────────────────┐
│ Upon first accessing a   │
│ secured area, receiving  │ ── 96
│ a user identification    │
└──────────────────────────┘
           │
           ▼
┌──────────────────────────┐
│ Replacing the globally   │
│ unique identifier as the │ ── 98
│ key to the database      │
│ entry with the user      │
│ identification           │
└──────────────────────────┘
           │
           ▼
┌──────────────────────────┐
│ Storing the user         │
│ identification and the   │ ──100
│ globally unique          │
│ identifier in the client │
│ identifier               │
└──────────────────────────┘
           │
           ▼
┌──────────────────────────┐
│ Storing the globally     │
│ unique identifier in the │ ──102
│ database entry as a      │
│ separate field           │
└──────────────────────────┘
```

It is readily seen from process block 96 that the disclosure of Figure 4 pertains only to accessing a secured area. Process block 98 shows that the GUID is _replaced_ by the user identification, and col. 7, lines 57-58 teaches that the _GUID is no longer used_ for database entry. Thus, the disclosure of Figure 4 of Koneru clearly does not show Applicants' Claim 1 feature of authcode cookie utilizations that are interspersed between session cookie utilizations.

(Appeal Brief Page 21 of 33)
Kou et al.— 09/810,288

PAGE 23/35 * RCVD AT 8/23/2005 4:55:33 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-6/26 * DNIS:2738300 * CSID:972 385 7766 * DURATION (mm-ss):08-00

Regarding Koneru, col. 8, lines 1-36, Figure 5 of Koneru, at block 110, shows that the user identification must be used first, to gain access to a database entry. The user identification may then be used to access secure area 78. If it is desired to access non-secure area 76, the client GUID is checked against a stored GUID, as shown by block 112. Access is provided to the non-secure area 76 if the two GUIDs match. However, it is clear that following such use of the GUID, there is no further use of the user identification in the effort to access non-secure area 76. Thus, the Figure 5 arrangement of Koneru does not teach that utilizations of the user identification are interspersed between utilizations of the GUID thereof. Accordingly, Figure 5 and related teachings of Koneru fail to show the Claim 1 recitation of utilizations of the authcode cookie that are interspersed between utilizations of the session cookie.

Claim 20 is directed to subject matter similar to that of Claim 1, and is considered to distinguish over Konetsu et al. for the same reasons given in support thereof.

B.3.   Conclusion

For at least all of the above reasons, Applicants respectfully submit that Konetsu et al. does not teach or suggest all of the features of Claims 1 and 20.

At least by virtue of their dependency on Claims 1 and 20, respectively, Konetsu et al. does not teach or suggest the features of dependent Claims 2-7, 21-26 and 29-30.

Accordingly, it is respectfully requested that the Board reverse the Examiner's final rejection of Claims 1-7, 20-26 and 29-30.

C. GROUND OF REJECTION 3 (Claims 8-9, 18-19, 27-28, 31 and 33)

Claims 8-9, 18-19, 27-28, 31 and 33 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,966,705 (Koneru et al.) in view of U.S. Patent No. 6,092,196 (Reiche).

These claims all depend from and further restrict independent claims 1, 12 and 20. The Reiche patent does not supply the deficiencies in Koneru et al. with respect to the independent claims, as discussed in detail above. Accordingly, for at least the reasons discussed above, Claims 8-9, 18-19, 27-28, 31 and 33 are not obvious in view of any combination of Koneru et al. and Reiche, and should be allowable in their present form.

Therefore, Claims 8-9, 18-19, 27-28, 31 and 33 are believed to patentably distinguish over Koneru et al. and Reiche, and any combination thereof, and it is respectfully requested that the Board reverse the Examiner's final rejection of these claims.

James O. Skarsten
Reg. No. 28,346
YEE & ASSOCIATES, P.C.
PO Box 802333
Dallas, TX 75380
(972) 385-8777

(Appeal Brief Page 23 of 33)
Kou et al.– 09/810,288

CLAIMS APPENDIX

The text of the claims involved in the appeal are:

1.   A method of secure session management and authentication between a web site and a web client, said web site having secure and non-secure web pages, said method comprising the steps of:

a) utilizing a non-secure communication protocol and a session cookie when said web client requests access to said non-secure web pages;

b) utilizing a secure communication protocol and creating an authcode cookie when said web client requests access to said secure web pages, so that utilizations of said authcode cookie are interspersed between utilizations of said session cookie, and at least some utilizations of said session cookie take place after utilizations of said authcode cookie.

2.   The method of claim 1, wherein said method also comprises the steps of:

c) requesting said session cookie from said web client whenever said web client requests access to said non-secure web pages and verifying said requested session cookie; and

d) requesting said authcode cookie from said web client whenever said web client requests access to said secure web pages and verifying said requested authcode cookie.

3.   The method of claim 2, wherein said method comprises repeatedly alternating between said secure communication protocol and said non-secure communication

protocol when said web client alternates requests for access to said secure web pages and said non-secure web pages, respectively, and also repeatedly alternating between said utilizations of said authcode and said utilizations of said session code.

4.   The method of claim 3, wherein said alternating between said secure communication protocol and said non-secure communication protocol is facilitated by a table which keeps track of said non-secure web pages and said secure web pages.

5.   The method of claim 4, wherein said web site uses said table to direct said web client to use said secure communication protocol or said non-secure communication protocol depending on whether said web client requests access to said non-secure web pages or said secure web pages.

6.   The method of claim 6, wherein said method also comprises allowing said web client to be a guest client or a registered client.

7.   The method of claim 6, wherein said method also comprises creating stored information including data contained in said session cookie, data contained in said authcode cookie and data about said web client.

8.   The method of claim 7, wherein said session cookie includes a pointer and an encrypted portion, said pointer pointing to said stored information, said encrypted portion having a random portion and a date portion.

9.   The method of claim 7, wherein said authcode cookie includes an encrypted portion, said encrypted portion having a random portion and a date portion.

10.   The method of claim 8, wherein verifying said requested session cookie from said web client includes using said stored information to generate a second session cookie and comparing said second session cookie to said session cookie requested from said web client.

11.   The method of claim 9, wherein verifying said requested authcode cookie from said web client includes using said stored information to generate a second authcode cookie and comparing said second authcode cookie to said authcode cookie requested from said web client.

12.   A system, for secure session management and authentication between a web site and a web client, said system comprising a web server, a web client and a communication channel, said web server coupled to said web client via said communication channel, said web server having a web site, said web site including:

a) secure and non-secure web pages;

b) a non-secure communication protocol and a session cookie that is used for allowing said web client access to each one of said non-secure web pages; and

c) a secure communication protocol and an authcode cookie that is used for allowing said web client access only to said secure web pages.

(Appeal Brief Page 26 of 33)
Kou et al.– 09/810,288

13.   The system of claim 12, wherein said web site also includes:

        d) verification means for verifying said session cookie when said session cookie is requested from said web client; and

        e) verification means for verifying said authcode cookie when said authcode cookie is requested from said web client.

14.   The system of claim 13, wherein said web server further comprises a security alternating means for alternating between said secure communication protocol and said non-secure communication protocol.

15.   The system of claim 14, wherein said web server further comprises a table to keep track of said non-secure web pages and said secure web pages.

16.   The system of claim 13, wherein said web site includes access means to allow said web client to access said web site as a guest client or a registered client.

17.   The system of claim 16, wherein said web system has storage means for containing stored information about said web client, data contained in said session cookie and data contained in said authcode cookie.

18.   The system of claim 17, wherein said session cookie includes a pointer and an encrypted portion, said pointer pointing to said stored information, said encrypted portion having a random portion and a date portion.

19.   The system of claim 17, wherein said authcode cookie includes an encrypted portion, said encrypted portion having a random portion and a date portion.

20.   A computer program embodied on a computer readable medium, said computer program providing for secure session management and authentication between a web site and a web client, said web site having secure and non-secure web pages, said computer program adapted to:

a) use a non-secure communication protocol and a session cookie when said web client requests access to said non-secure web pages;

b) use a secure communication protocol and an authcode cookie whenever said web client requests access to said secure web pages.

21.   The computer program of claim 20, wherein said computer program is further adapted to:

c) request said session cookie from said web client when said web client requests access to said non-secure web pages and to verify said requested session cookie; and

d) request said authcode cookie from said web client when said web client requests access to said secure web pages and to verify said requested authcode cookie.

22.   The computer program of claim 21, wherein said computer program is further adapted to alternate between said secure communication protocol and said non-secure communication protocol when said web client alternates requests for access to said secure web pages and said non-secure web pages.

23.   The computer program of claim 22, wherein said alternating between said secure communication protocol and said non-secure communication protocol is facilitated by a table which keeps track of said non-secure web pages and said secure web pages.

24.   The computer program of claim 23, wherein said computer program uses said table to direct said web client to use said secure communication protocol or said non-secure communication protocol depending on whether said web client requests access to said non-secure web pages or said secure web pages.

25.   The computer program of claim 22, wherein said computer program is adapted to allow said web client to be a guest client or a registered client.

26.   The computer program of claim 25, wherein said computer program is adapted to create stored information including data contained in said session cookie, data contained in said authcode cookie and data about said web client.

27.   The computer program of claim 26, wherein said session cookie includes a pointer and an encrypted portion, said pointer pointing to said stored information, said encrypted portion having a random portion and a date portion.

28.   The computer program of claim 26, wherein said authcode cookie includes an encrypted portion, said encrypted portion having a random portion and a date portion.

29.   The computer program of claim 27, wherein verifying said requested session cookie from said web client includes using said stored information to generate a second session cookie and comparing said second session cookie to said session cookie requested from said web client.

30.   The computer program of claim 28, wherein verifying said requested authcode cookie from said web client includes using said stored information to generate a second authcode cookie and comparing said second authcode cookie to said authcode cookie requested from said web client.

31.   The computer program of Claim 20, wherein said computer program is adapted to create a NAME attribute in a session cookie:

   a) generating a user_id;

   b) generating a session_string;

   c) generating a session_timestamp;

d) appending said session_timestamp to said session_string to create an intermediate value;

e) applying a one way hash function to said intermediate value to create a final value; and

f) storing said final value in said NAME attribute.

32.   (Canceled)

33.   The computer program of Claim 20, wherein said computer program is adapted to create a NAME attribute in an authcode cookie by:

a) generating an authcode;

b) generating an authcode_timestamp;

c) appending said authcode_timestamp to said authcode to create an intermediate value;

d) applying a one way hash function to said intermediate value to create a final value; and

e) storing said final value in said NAME attribute.

34.   (Canceled)

EVIDENCE APPENDIX

There is no evidence to be presented.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings.